UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/614,901	07/09/2003	Hidetoshi Fujimoto	01-445	1869

23400 7590 03/22/2007	EXAMINER
POSZ LAW GROUP, PLC 12040 SOUTH LAKES DRIVE SUITE 101 RESTON, VA 20191	AGWUMEZIE, CHARLES C

ART UNIT	PAPER NUMBER
3621	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/614,901	FUJIMOTO ET AL.
	Examiner	Art Unit	
	Charlie C. Agwumezie	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 July 2003</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All   b)☐ Some *   c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>7/9/03; 9/8/05</u>. 11/1/05, 2/14/06

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 8-14, are rejected under 35 U.S.C. 102(b) as being anticipated by

Kawano et al U.S. Patent No. 5,995,623.

As per **claim 8**, Kawano et al discloses a decryption method for decrypting

decryption target data based on an encryption rule that is applied to encryption of

encryption target data for producing the decryption target data, comprising steps of:

dividing the decryption target data into decryption target units (fig. 6; col. 9, lines

45-65; col. 14, lines 1-15;...providing a different encryption method for each data to be

encrypted...); and

decrypting each of the decryption target units based on a decryption ratio of

actually decrypted data length, within the each of the decryption target units, to entire

data length of the each of the decryption target units (see fig. 6; col. 9, lines 45-60; col.

13, lines 45-65),

wherein the entire data length of the each of the decryption target units does not

change both prior to and subsequent to being decrypted (see figs. 6D, 6E; col. 12, lines

30-40).

As per **claim 9**, Kawano et al further discloses the decryption method, wherein the decryption ratio includes a plurality of different kinds, and wherein each of the plurality of different kinds of the decryption ratio is applied, in certain order, for decrypting (fig. 6; col. 9, lines 45-65; col. 14, lines 1-15; ...providing a different encryption method for each data to be encrypted...).

As per **claim 10**, Kawano et al further discloses the decryption method, wherein, when a certain kind of the decryption ratio is applied in the certain order, the certain kind of the decryption ratio is repeatedly applied for decrypting, at a certain number of times (see fig. 6; col. 15, lines 5-15).

As per **claim 11**, Kawano et al further discloses the decryption method, wherein, when the each of the decryption target units is decrypted based on the decryption ratio, decryption of the each of the decryption target units starts from a decryption starting point that is located in a certain point within the each of the decryption target units (see fig. 6).

As per **claim 12**, Kawano et al further discloses the decryption method, wherein the decryption starting point includes a plurality of different kinds, wherein a plurality of decryption patterns are generated by combination of the plurality of different kinds of the decryption ratio with the plurality of different kinds of the decryption starting point, and

wherein each of the plurality of decryption patterns is applied, in given order, for

decrypting (see figs. 6 and 8; col. col. 14, lines 1-15; ...providing a different encryption

method for each data to be encrypted...).

As per **claims 13 and 14**, Kawano et al discloses a data decryption device for

decrypting decryption target data based on an encryption rule that is applied to

encryption of encryption target data for producing the decryption target data,

comprising:

an inputting module for inputting the decryption target data (see figs. 8, 10, 13

and 15);

a decrypting module for decrypting the inputted decryption target data (figs. 1, 6,

and 7); and

an outputting module for outputting the decrypted decryption target data, wherein

the decrypting module includes:

dividing means for dividing the decryption target data into decryption target units

(fig. 6; col. 9, lines 45-65; col. 14, lines 1-15;...providing a different encryption method

for each data to be encrypted...); and

decrypting means for decrypting each of the decryption target units based on a

decryption ratio of actually decrypted data length, within the each of the decryption

target units, to entire data length of the each of the decryption target units (see fig. 6;

col. 9, lines 45-60; col. 13, lines 45-65),

wherein the entire data length of the each of the decryption target units does not change

both prior to and subsequent to being decrypted (see figs. 6D, 6E; col. 12, lines 30-40).

Claim Rejections - 35 USC § 103

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, and 7-8, are rejected under 35 U.S.C. 103(a) as being unpatentable

over Raley et al U.S. Patent Application Publication No. 2003/0177400 A1 in view of

Kawano et al U.S. Patent No. 5,995,623.

As per **claims 1**, Raley et al discloses an encryption method for encryption target

data, comprising steps of:

dividing the encryption target data into encryption target units (0022; 0096; see

claim 1, 6); and

encrypting each of the encryption target units based on an encryption ratio of

actually encrypted data length, within the each of the encryption target units, to entire

data length of the each of the encryption target units (0022; see claims 1, 2, 6 and 7;

"...encrypting one or more portions of data based on the encryption ratio..."),

wherein the entire data length of the each of the encryption target units does not

change both prior to and subsequent to being encrypted.

What Raley et al does not explicitly teach is wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted.

Kawano et al discloses wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted (see figs. 6D, 6E; col. 12, lines 30-40)

Accordingly it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the system of Raley et al and incorporate a method wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted in view of the teachings of Kawano et al in order to further ensure security.

As per **claims 2 and 9**, Raley et al further discloses the encryption method, wherein the encryption ratio includes a plurality of different kinds, and wherein each of the plurality of different kinds of the encryption ratio is applied, in certain order, for encrypting (0095; 0096; ...encryption can vary between values specified...).

As per **claims 3 and 10**, Raley et al further discloses the encryption method, wherein, when a certain kind of the encryption ratio is applied in the certain order, the certain kind of the encryption ratio is repeatedly applied for encrypting, at a certain number of times (0095; 0096).

As per **claims 4 and 11**, Raley et al further discloses the encryption method, wherein, when the each of the encryption target units is encrypted based on the encryption ratio, encryption of the each of the encryption target units starts from an encryption starting point that is located in a certain point within the each of the encryption target units (0022; 0095; 0096).

As per **claim 5**, Raley et al further discloses the encryption method, wherein the encryption starting point includes a plurality of different kinds, wherein a plurality of encryption patterns are generated by combination of the plurality of different kinds of the encryption ratio with the plurality of different kinds of the encryption starting point, and wherein each of the plurality of encryption patterns is applied, in given order, for encrypting (0022; 0096; ...encrypts portions of the documents...divided by time intervals or based on the byte size...).

As per **claims 6, and 7**, Raley et al discloses an data encryption device for encrypting encryption target data, comprising:

an inputting module for inputting the encryption target data (fig. 1, 3);

an encrypting module for encrypting the inputted encryption target data (fig. 1, 15); and

an outputting module for outputting the encrypted encryption target data, wherein the encrypting module includes:

dividing means for dividing the inputted encryption target data into encryption target units (0022; 0096; see claim 1, 6); and

encrypting means for encrypting each of the encryption target units based on an encryption ratio of actually encrypted data length, within the each of the encryption target units, to entire data length of the each of the encryption target units (0022; see claims 1, 2, 6 and 7; "...encrypting one or more portions of data based on the encryption ratio..."),

wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted.

What Raley et al does not explicitly teach is wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted.

Kawano et al discloses wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted (see figs. 6D, 6E; col. 12, lines 30-40)

Accordingly it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the system of Raley et al and incorporate a method wherein the entire data length of the each of the encryption target units does not change both prior to and subsequent to being encrypted in view of the teachings of Kawano et al in order to further ensure security.

Conclusion

3.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure. The reference cited to Liu et al et al U.S. Patent 5,539,827 is

document considered relevant to the claimed invention.

Examiner's Note: Examiner has cited particular columns and line numbers in

the references as applied to the claims below for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art ad are

applied to the specific limitations within the individual claim, other passages and figures

may apply as well. It is respectfully requested that the applicant, in preparing the

responses, fully consider the references in entirety as potentially teaching all or part of

the claimed invention, as well as the context of the passage as taught by the prior art or
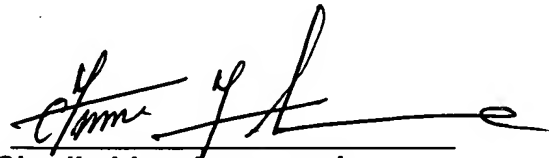
disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Charles C. Agwumezie whose number is **(571) 272-**

6838. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Andrew Fischer can be reached on **(571) 272 – 6779**.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Charlie Lion Agwumezie
Patent Examiner
Art Unit 3621

Acc
March 16, 2007

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600